UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,400	08/14/2006	Tsuyoshi Kasaura	1190-0634PUS1	7042

2292 7590 07/16/2008
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
07/16/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/589,400	KASAURA ET AL.	
	Examiner	Art Unit	
	AMARE TABOR	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 August 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This correspondence is in response to **Amendments** and **REMARKS** filed on March 17, 2008.

2. Claims 1, 4, 7 and 11 are amended; Claims 2, 3, 5, 6, 8-10 and 12-14 are original; and Claim 15 is new.

3. **Claims 1-15** are pending.

Response to Arguments

4. Applicant's arguments with respect to the pending claims have been considered but are moot in view of the new ground(s) of rejection.

Specification

5. The amendment filed on 03/17/2008 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

- amended independent **claims 1 and 4** recite, "*...a control section which performs a **dynamic** process of issuing the digital certificate...*"; and,
- newly added **claim 15** recite, "*A computer readable storage medium ... for performing a dynamic process of issuing the digital certificate through a wired connection means creating a network ...*"

However, the disclosure invention does not disclose control section and/or computer readable storage medium dynamically issuing digital certificate.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balfanz et al (US 2003/0149874 A1, referred as "Balfanz") in view of Hind et al. (US 6, 772, 331 B1, referred as "Hind"), and further in view of Vilhuber et al. (US 7,386,721 B1, referred as "Vilhuber")

As per Claim 1, Balfanz teaches,

A data sending/receiving device (see *310* in *Fig.* 3) for issuing a digital certificate (see *PK1 at step S110 of Fig. 5*) to a new data sending/receiving device (see *320* in *Fig.* 3), when the data sending/receiving device causes the new data sending/receiving device to participate in a network formed by data sending/receiving devices (see *abstract; Fig. 2;* and for example, paragraph [0002] and [0010]) and each having a digital certificate (see *PK1 & PK2* in *Fig.* 5) that certifies authority to participate in the network (see *step S160* in *Fig. 5*); the data sending/receiving device comprising:

a first communication section which performs communication in the network (see *314 & 324* in *Fig. 3;* and *MAIN WIRELESS LINK INTERFACE 434* in *Fig. 4*);

a second communication section, to which the new data sending/receiving device can be connected (see *312 & 322* in *Fig. 3;* and *LOCATION-LIMITED CHANNEL INTERFACE 432* in *Fig. 4*);

and a control section which performs a process of issuing the digital certificate (see *AUTHENTICATION PROGRAM 426* and *AUTHENTICATOR 428* in *Fig. 4*);

wherein when the new data sending/receiving device is connected to the second communication section, the control section judges whether or not the new data sending/receiving device is a device having a communication means that can communicate in the network, in accordance with device type

information of the new data sending/receiving device received via the second communication section from the new data sending/receiving device (see *Fig. 3;* and for example, paragraph [0033]-[0036]), and

if the new data sending/receiving device is judged as a device having a communication means that can communicate in the network the created digital certificate is sent via the second communication section to the new data sending/receiving device (see *Fig. 5; where at steps S110-120 PK1 and PK2 are sent using a location-limited channel 432 of Fig. 4*).

Balfanz fails to teach explicitly the control section creates the digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device, the device identifier being received via the second communication section from the new data sending/receiving device.

However, in the same field of endeavor, Hind teaches creating digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device (see *abstract* and *Device Certificate 1050 -including Device Identifier 4010* in *Fig. 4*), the device identifier being received via the second communication section from the new data sending/receiving device (see *Fig. 3;* and for example, column 1, lines 17-21 and column 6, lines 10-25).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicant's invention to combine the teachings of Hind and to the system of Balfanz because both are in the fields of securing a network communication channel between devices using public key cryptography. Incorporating Hind's teaching creating a digital certificate by using a device identifier modifies the system of Belfaz. The modification benefits to distinctly identify the second device that would require a secure communication with the first device of an enterprise [see column 2, lines 11-54 of **Hind**].

Belfaz-Hind combination teaches a second communication section and a control section issuing digital certificate [see FIGS.3 and 4 of **Belfaz**]; but fails to disclose the communication section connected by a wired connection means, and the control section dynamically issuing digital certificate through the

wired connection means to enable a secure communication protocol before the creation of the digital certification for the individual digital certificate.

Nevertheless, in the same field of endeavor, Vilhuber discloses the communication section connected by a wired connection means [see **CONFIGURATION SERVER 102, NETWORK DEVICE 104** and **PROVISIONING ENVIRONMENT 106** in FIG.1; and for example, col.1, lines 27-40, "*… configuration server 102 is selectively communicatively coupled to one or more network devices 104…accessible through a provisioning environment 106, which provides a physical mounting location for the network devices, power supplies, … for connectivity to network 108…*"], and the control section dynamically issuing digital certificate through the wired connection means to enable a secure communication protocol before the creation of the digital certification for the individual digital certificate [see for example, abstract, "*…In one embodiment, the identity certification module is configured to generate a digital certificate for the network device and the configuration module is configured to automatically configure the network device based on its digital certificate. The provisioning server is coupled to the network device with a secure communication link*"].

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of Applicant's invention, to modify Belfaz-Hind combination by incorporating the communication section of Vilhuber in order to deploy a more trusted network device into its network operation [see abstract of **Vilhuber**].

As per Claim 4, Balfanz teaches,

A data sending/receiving device (see *310* in *Fig.* 3) for issuing a digital certificate (see *PK1 at step S110 of Fig. 5*) to a new data sending/receiving device (see *320* in *Fig.* 3), when the data sending/receiving device causes the new data sending/receiving device to participate in a network formed by data sending/receiving devices (see *abstract; Fig. 2;* and for example, paragraph [0002] and [0010]) each having a digital certificate that certifies authority to participate in the network (see *PK1 & PK2* and *step S160* in *Fig.* 5); the data sending/receiving device comprising:

a communication section which performs communication in the network (see *314 & 324* in *Fig. 3;* and *MAIN WIRELESS LINK INTERFACE 434* in *Fig. 4*); and

a control section which performs a process of issuing the digital certificate (see *AUTHENTICATION PROGRAM 426* and *AUTHENTICATOR 428* in *Fig. 4*); wherein

if the new data sending/receiving device is judged as a device having a communication means that can communicate in the network, the control sends the created digital certificate via the communication section (see *Fig. 3;* and for example, paragraph [0033]-[0036]) and via the data sending/receiving device to which the new data sending/receiving device is connected (see *Fig. 5; where at steps S110-120 PK1 and PK2 are sent using a location-limited channel 432 of Fig. 4*).

Balfanz fails to teach explicitly the control section creates a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device; however, Hind teaches creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device (see *Fig. 3, abstract* and *Device Identifier 4010* in *Fig. 4;* and for example, column 1, lines 17-21 and column 6, lines 10-25).

It would have been obvious to a person having ordinary skill in the art at the time of Applicant's invention to create a digital certificate by using a device identifier as taught by Hind in order to distinctly identify the second device that would require a secure communication with the first device [see BACKGROUND of **Hind**].

Belfaz-Hind combination teaches a control section issuing digital certificate [see FIGS.3 and 4 of **Belfaz**]; but fails to disclose the control section dynamically issuing dynamic digital certificate through the wired connection means to enable a secure communication protocol before the creation of the digital certification for the individual digital certificate.

Nevertheless, Vilhuber discloses the control section dynamically issuing dynamic digital certificate through the wired connection means to enable a secure communication protocol before the creation of the digital certification for the individual digital certificate [see abstract, **CONFIGURATION SERVER 102,**

NETWORK DEVICE 104 and **PROVISIONING ENVIRONMENT 106** in FIG.1; and for example, col.1, lines 27-40].

It would have been obvious to a person of ordinary skill in the art, at the time of Applicant's invention, to modify Belfaz-Hind combination by incorporating the control section of Vilhuber in order to deploy a more trusted network device into its network operation [see abstract of **Vilhuber**].

As per Claim 7, Balfanz teaches,

A digital certificate issuing method (see *Fig. 5* and *abstract*) for issuing a digital certificate (see *PK1 at step S110 of Fig. 5*) to a new data sending/receiving device (see *320* in *Fig.* 3) when the new data sending/receiving device participates in a network formed by a plurality of data sending/receiving devices each having a digital certificate that certifies authority to participate in the network (see *Fig. 2 & 5;* and for example, paragraph [0002] and [0010]), the method comprising the steps of:

judging by a certain data sending/receiving device, whether or not the new data sending/receiving device is a device having a communication means that can communicate in the network in accordance with device type information of the new data sending/receiving device received from the new data sending/receiving device; and the new data sending/receiving device is judged as being a device having a communication means that can communicate in the network (see *Fig. 3;* and for example, paragraph [0033]-[0036]).

Balfanz fails to teach explicitly creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device received from the new data sending/receiving device and sending the created digital certificate to the new data sending/receiving device, by the certain data sending/receiving device.

However, Hind teaches creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device received from the new data sending/receiving device and sending the created digital certificate to the new data sending/receiving

device, by the certain data sending/receiving device (see *Fig. 3, abstract* and *Device Identifier 4010* in *Fig. 4;* and for example, column 1, lines 17-21 and column 6, lines 10-25).

It would have been obvious to a person having ordinary skill in the art at the time of Applicant's invention to create a digital certificate by using a device identifier as taught by Hind in order to distinctly identify the second device that would require a secure communication with the first device [see BACKGROUND of **Hind**].

Belfaz-Hind combination fails to disclose connecting the new data sending/receiving device through a wired connection means to a certain data sending/receiving device participating in the network in order to enable a secure communication protocol before the creation of the digital certification for the individual digital certificate.

Nevertheless, Vilhuber discloses connecting the new data sending/receiving device through a wired connection means to a certain data sending/receiving device participating in the network in order to enable a secure communication protocol before the creation of the digital certification for the individual digital certificate [see abstract, **CONFIGURATION SERVER 102, NETWORK DEVICE 104** and **PROVISIONING ENVIRONMENT 106** in FIG.1; and for example, col.1, lines 27-40].

It would have been obvious to a person of ordinary skill in the art, at the time of Applicant's invention, to modify Belfaz-Hind combination by incorporating Vilhuber's teaching in order to deploy a more trusted network device into its network operation [see abstract of **Vilhuber**].

As per Claim 11, Balfanz teaches,

A digital certificate issuing method (see *Fig. 5* and *abstract*) for issuing a digital certificate to (see *PK1 at step S110 of Fig. 5*) a new data sending/receiving device (see *320* in *Fig.* 3) when the new data sending/receiving device participates in a network formed by a plurality of data sending/receiving devices each having a digital certificate that certifies authority to participate in the network (see *Fig. 2 & 5;* and for example, paragraph [0002] and [0010]), the method comprising the steps of:

judging, by one of the data sending/receiving devices forming the network, whether or not the new data sending/receiving device is a device having a communication means that can communicate in the network in accordance with device type information of the new data sending/receiving device received from the new data sending/receiving device; and the one of the data sending/receiving devices forming the network, which is other than the data sending/receiving device to which the new data sending/receiving device is connected through the wired connection means, judges that the new data sending/receiving device is judged as being a device having a communication means that can communicate in the network (see *Fig. 3;* and for example, paragraph [0033]-[0036]).

Balfanz fails to teach explicitly creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device received via the data sending/receiving device, to which the new data sending/receiving device is connected.

However, Hind teaches creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device received via the data sending/receiving device, to which the new data sending/receiving device is connected (see *abstract* and *Device Certificate 1050 -including Device Identifier 4010* in *Fig. 3 & 4;* and for example, column 1, lines 17-21 and column 6, lines 10-25).

It would have been obvious to a person having ordinary skill in the art at the time of Applicant's invention to create a digital certificate by using a device identifier as taught by Hind in order to distinctly identify the second device that would require a secure communication with the first device of an enterprise (see BACKGROUND of Hind).

Belfaz-Hind combination fails to disclose connecting the new data sending/receiving device through a wired connection means to a certain data sending/receiving device participating in the network in order to enable a secure communication protocol before the creation of the digital certification for the individual digital certificate.

Nevertheless, Vilhuber discloses connecting the new data sending/receiving device through a wired connection means to a certain data sending/receiving device participating in the network in order to enable a secure communication protocol before the creation of the digital certification for the individual digital certificate [see abstract, **CONFIGURATION SERVER 102, NETWORK DEVICE 104** and **PROVISIONING ENVIRONMENT 106** in FIG.1; and for example, col.1, lines 27-40].

It would have been obvious to a person of ordinary skill in the art, at the time of Applicant's invention, to modify Belfaz-Hind combination by incorporating Vilhuber's teaching in order to deploy a more trusted network device into its network operation [see abstract of **Vilhuber**].

As per Claim 15, Balfanz-Hind-Vilhuber combination teaches,

A computer readable storage medium having thereon computer executable program for performing a dynamic process of issuing the digital certificate through a wired connection means creating a network [see abstract, **CONFIGURATION SERVER 102, NETWORK DEVICE 104** and **PROVISIONING ENVIRONMENT 106** in FIG.1; and for example, col.1, lines 27-40 of **Vilhuber**], the computer program when executed causes a processor to execute steps of: judging by a certain data sending/receiving device that is one of the data sending/receiving devices forming the network and is connected through a wired connection means to the new data sending/receiving device, whether or not the new data sending/receiving device is a device having a communication means that communicates in the network in accordance with device type information having the new data sending/receiving device received from the new data sending/receiving device [see *Fig. 3;* and for example, paragraphs 0033-0036 of **Belfanz**]; and

if the new data sending/receiving device is judged as being a device having a communication means that can communicate in the network, creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device received from the new data sending/receiving device and sending the created digital certificate to the new data sending/receiving device, by the certain data sending/receiving device [see *abstract* and *Device Certificate 1050 -including Device Identifier 4010* in *Fig. 3 & 4;* and for example, column 1, lines 17-21

and column 6, lines 10-25 of **Hind**].

As per Claims 2, 5, 8 and 12, Balfanz-Hind-Vilhuber combination teaches,

wherein even when the new data sending/receiving device is judged as being the device having the communication means which can participate in the network, if the new data sending/receiving device already has a digital certificate (see *PK2* in *Fig. 5* of ***Belfaz***), the control section does not issue a new digital certificate (*since the second device 320* of *Fig. 3 have a public key PK2, a new digital certificate will not be issued*).

As per Claims 3, 6, 9 and 13, Balfanz-Hind-Vilhuber combination teaches,

wherein even when the new data sending/receiving device is judged as being the device having the communication means which can participate in the network and the new data sending/receiving device already has a digital certificate (see *PK2* in *fig. 5* of ***Belfaz***), if the digital certificate that is already held in the new data sending/receiving device is for another network different from the network (see *340* in *Fig. 3* and *MAIN WIRELESS LINK RX/TX 444* in *Fig. 4;* and for example, paragraphs [0037], [0039] to [0041] and [0047] of ***Belfaz***).

Hind teaches creating a digital certificate for the new data sending/receiving device by using the device identifier and sends the created digital certificate to the new data sending/receiving device are performed (see *abstract* and *Device Identifier 4010* in *Fig. 3 & 4;* and for example, column 1, lines 17-21 and column 6, lines 10-25).

As per Claims 10 and 14, Balfanz-Hind-Vilhuber combination teaches,

wherein the new data sending/receiving device verifies validity of the received digital certificate (see *AUTHENTICATION PROGRAM 424* and *AUTHENTICATOR 428* in *Fig. 4; where* ***Belfaz*** *discloses verifying the validity of the public key certificate*),

if it is confirmed that the validity exists, the new data sending/receiving device notifies the data sending/receiving device which has issued the digital certificate that the digital certificate has been accepted (see *steps S150-160* in *Fig. 5 of* ***Belfaz***), and

if it is not confirmed that the validity exists, the new data sending/receiving device requests the data sending/receiving device which has issued the digital certificate to issue a digital certificate again *RESUME COMMUNICATION S170* in *Fig. 5 of* ***Belfaz***).

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139